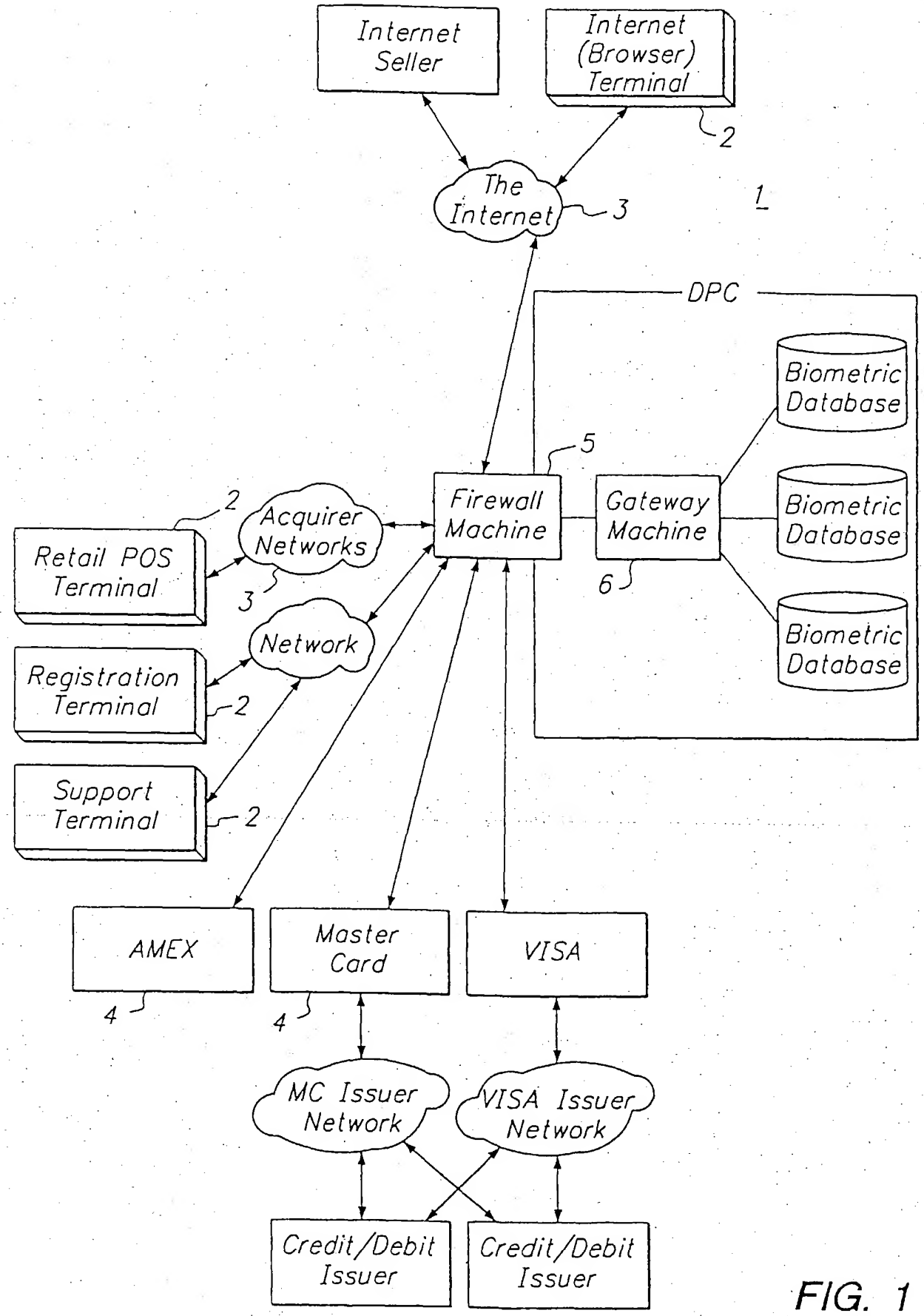
Internet Seller
Internet (Browser) Terminal
2
The Internet
3
1
DPC
Biometric Database
Biometric Database
Biometric Database
5
Firewall Machine
Gateway Machine
6
2
Acquirer Networks
3
Retail POS Terminal
Network
Registration Terminal
2
Support Terminal
2
AMEX
4
Master Card
4
VISA
MC Issuer Network
VISA Issuer Network
Credit/Debit Issuer
Credit/Debit Issuer

FIG. 1

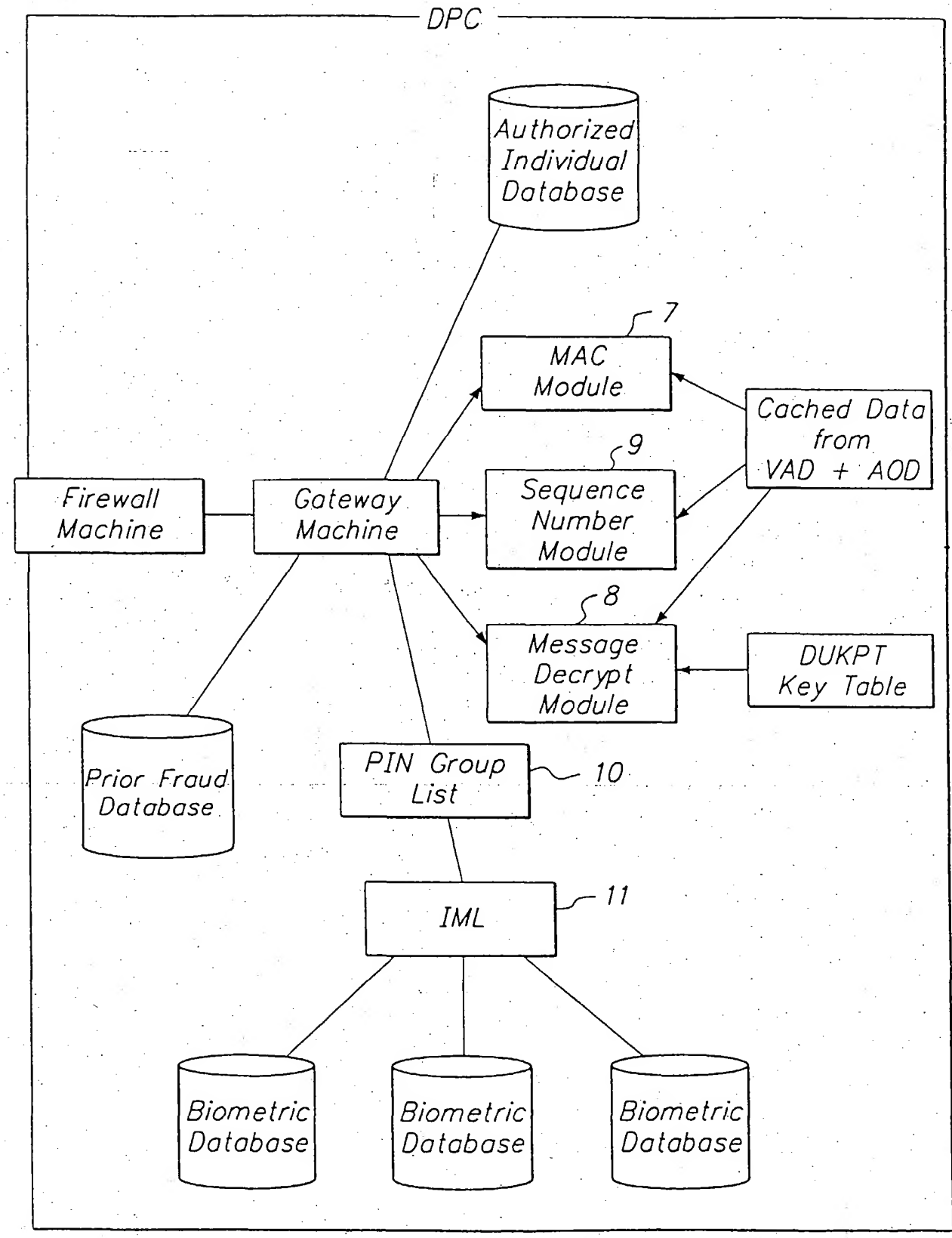
DPC
Authorized Individual Database
7
MAC Module
Cached Data from VAD + AOD
9
Sequence Number Module
Firewall Machine
Gateway Machine
8
Message Decrypt Module
DUKPT Key Table
Prior Fraud Database
PIN Group List
10
IML
11
Biometric Database
Biometric Database
Biometric Database

FIG. 2

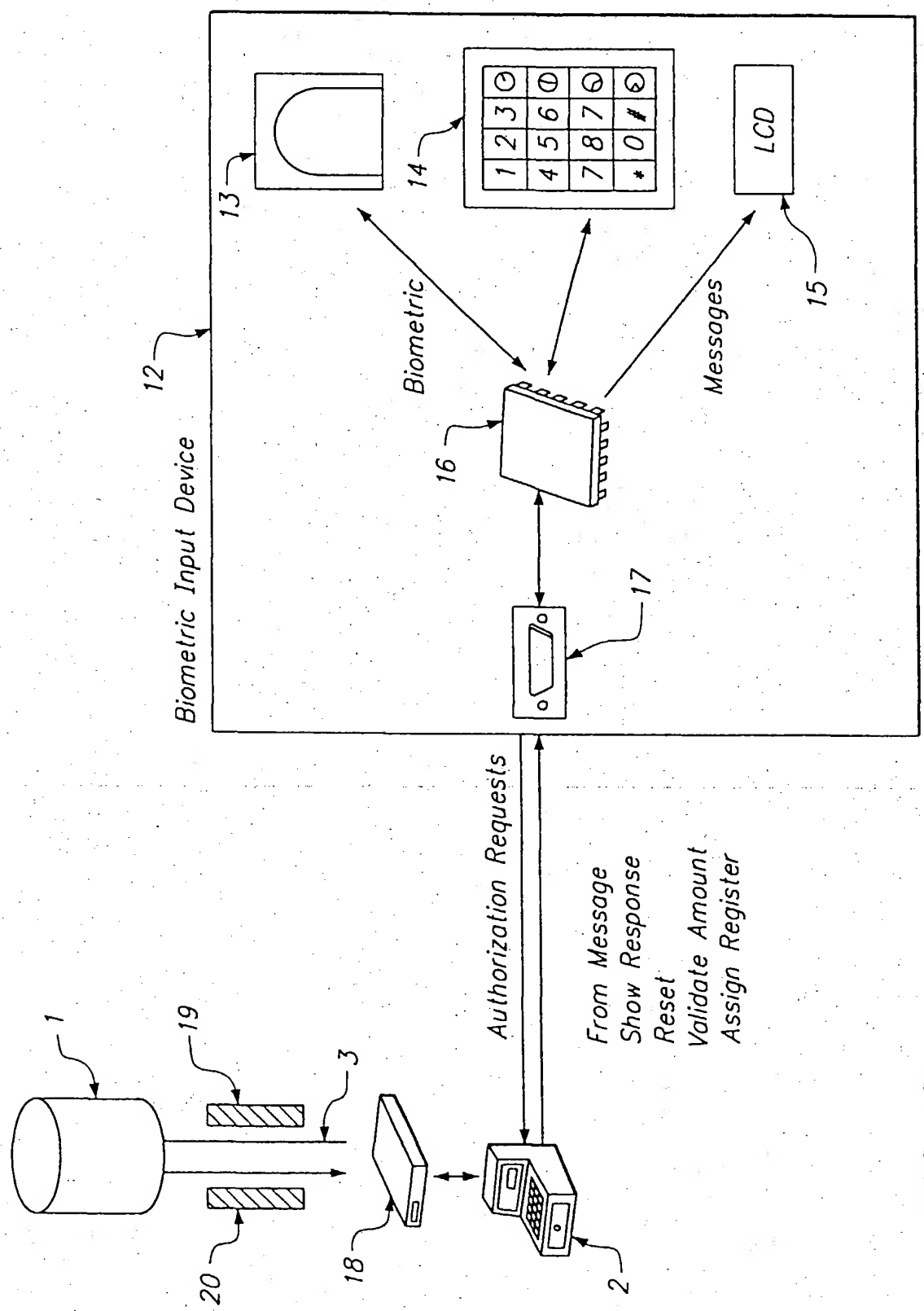
Biometric Input Device
12
13
14
1 2 3
4 5 6
7 8 9
* 0 #
LCD
15
Biometric
Messages
16
17
Authorization Requests
From Message
Show Response
Reset
Validate Amount
Assign Register
1
19
3
20
18
2

FIG. 3

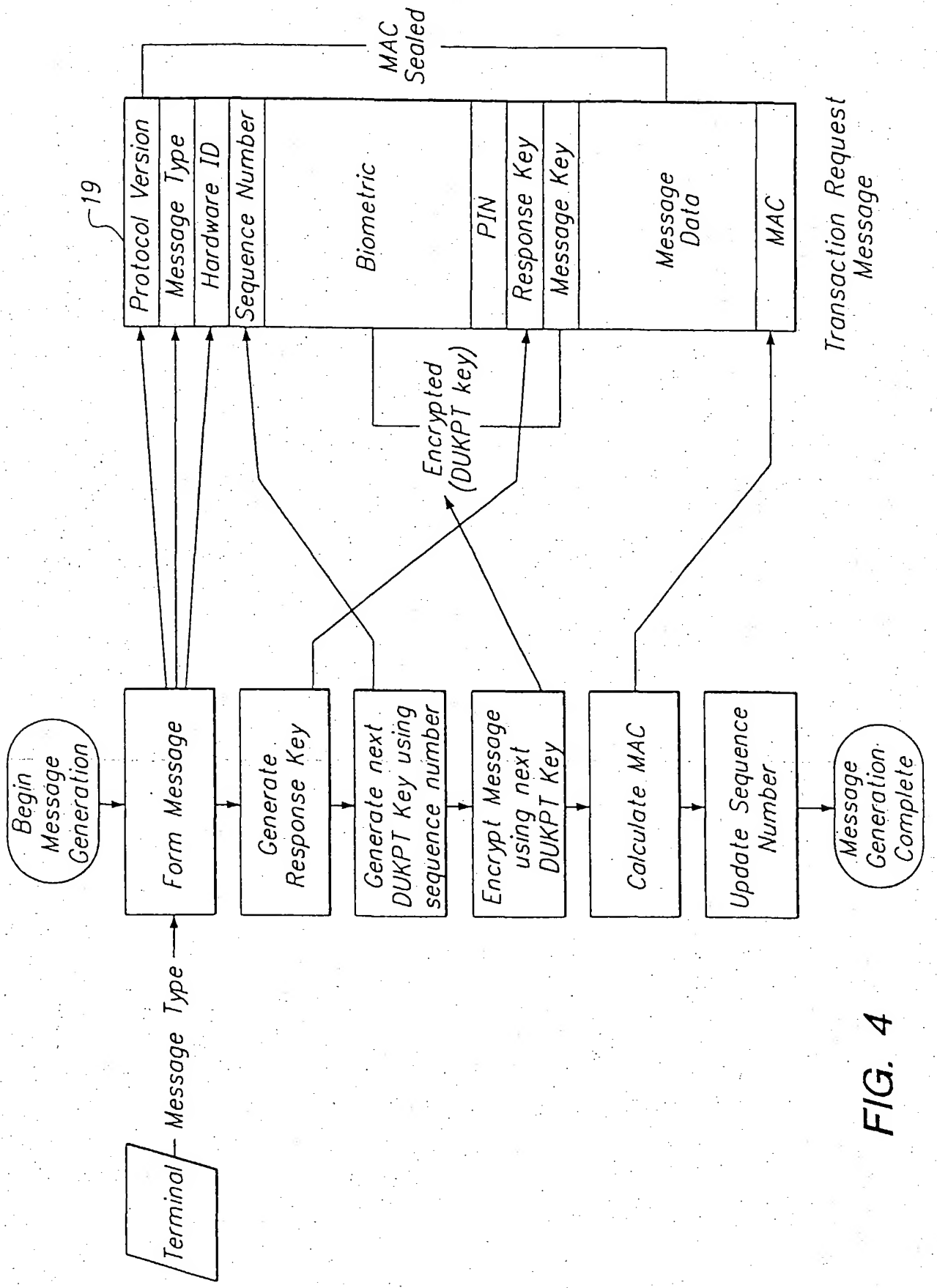
Terminal
Message Type
Begin Message Generation
Form Message
Generate Response Key
Generate next DUKPT Key using sequence number
Encrypt Message using next DUKPT Key
Calculate MAC
Update Sequence Number
Message Generation Complete
19
Protocol Version
Message Type
Hardware ID
Sequence Number
Biometric
PIN
Response Key
Message Key
Message Data
MAC
MAC Sealed
Encrypted (DUKPT key)
Transaction Request Message

FIG. 4

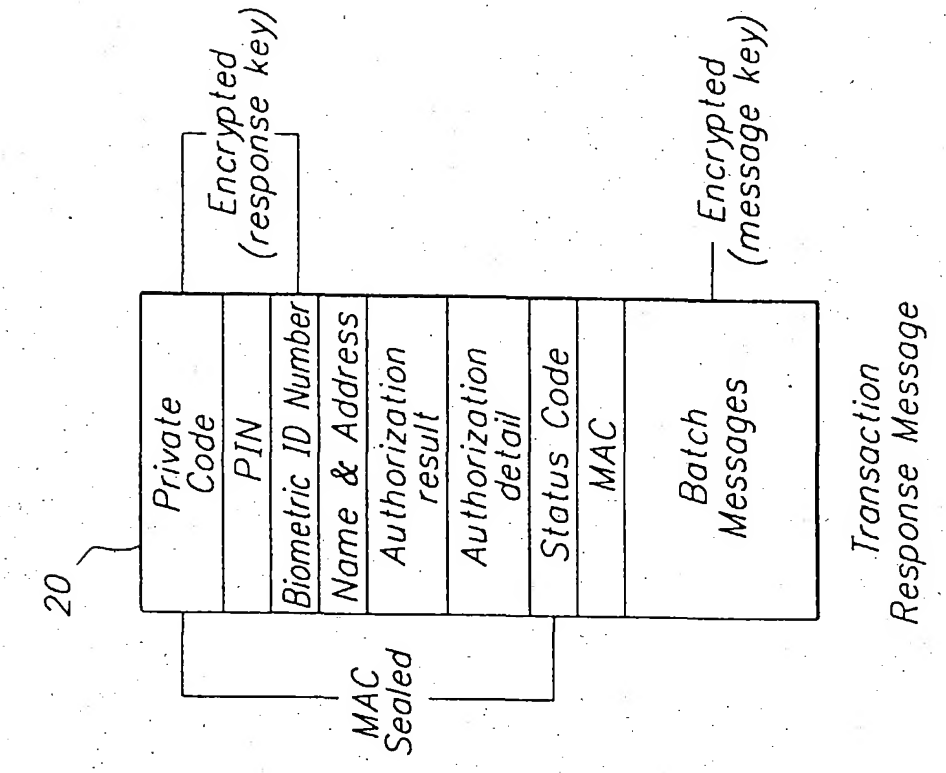
20
Private Code
PIN
Biometric ID Number
Name & Address
Authorization result
Authorization detail
Status Code
MAC
Batch Messages
Encrypted (response key)
Encrypted (message key)
MAC Sealed
Transaction Response Message

FIG. 6

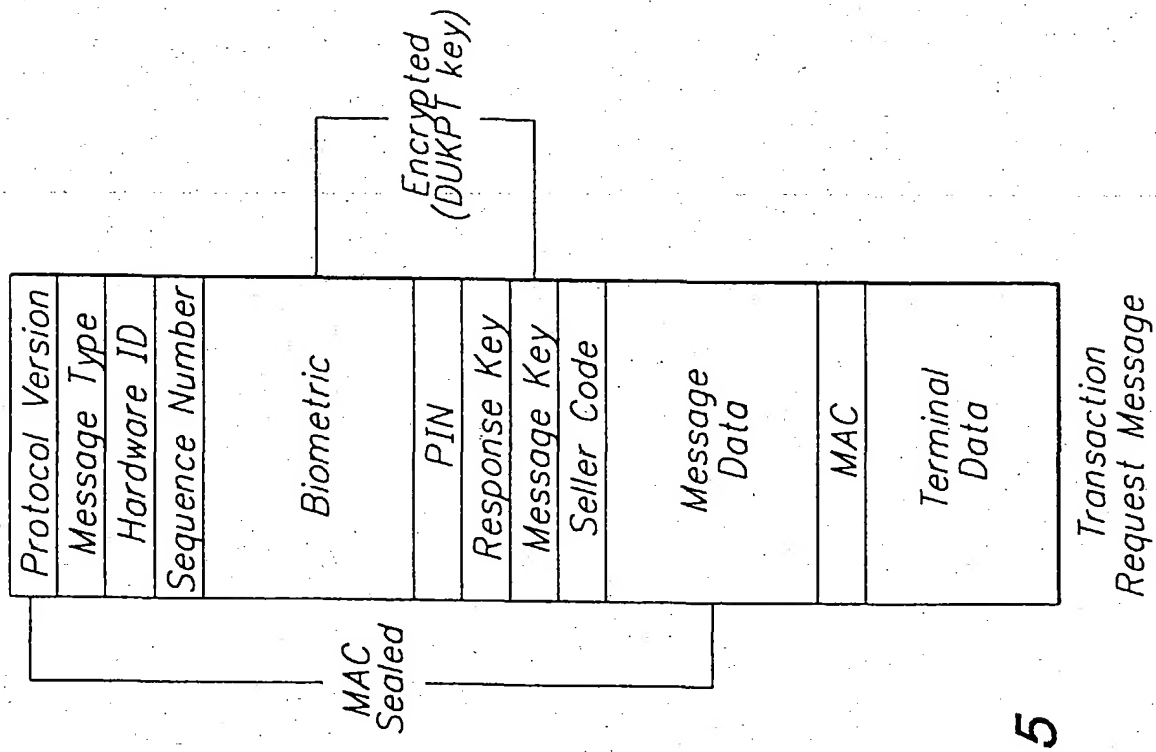
Protocol Version
Message Type
Hardware ID
Sequence Number
Biometric
PIN
Response Key
Message Key
Seller Code
Message Data
MAC
Terminal Data
Encrypted (DUKPT key)
MAC Sealed
Transaction Request Message

FIG. 5

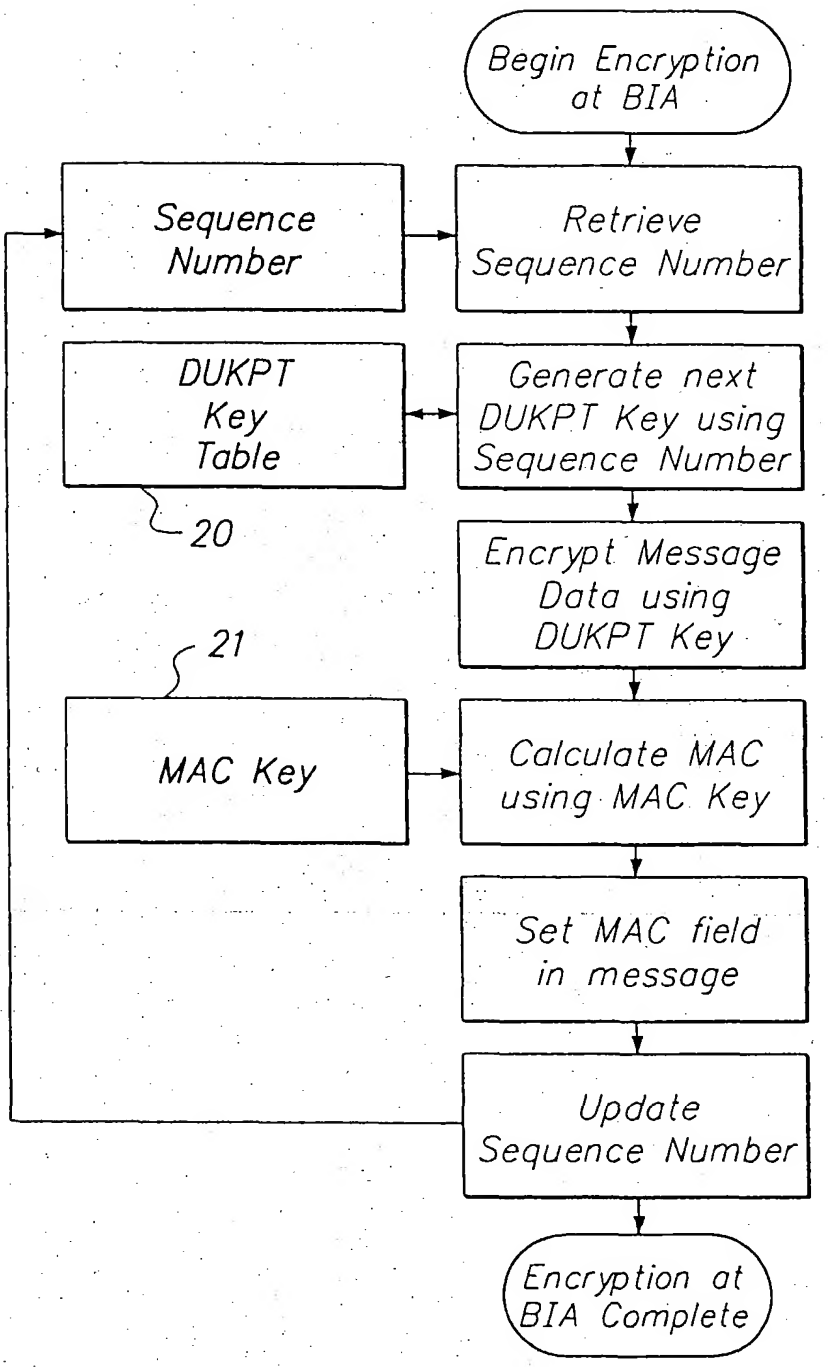
Begin Encryption at BIA
Sequence Number
Retrieve Sequence Number
DUKPT Key Table
Generate next DUKPT Key using Sequence Number
20
Encrypt Message Data using DUKPT Key
21
MAC Key
Calculate MAC using MAC Key
Set MAC field in message
Update Sequence Number
Encryption at BIA Complete

FIG. 7

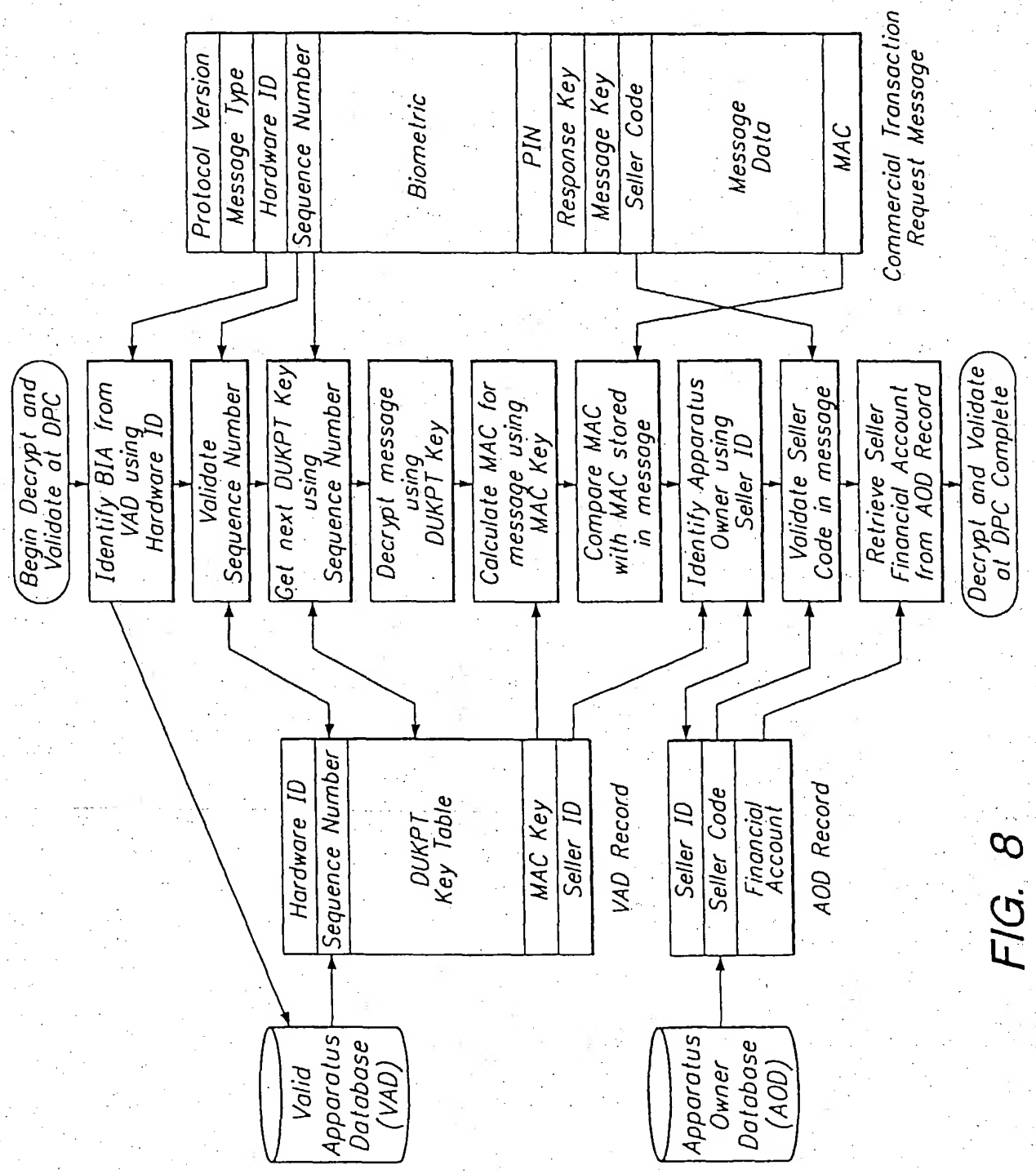
Protocol Version
Message Type
Hardware ID
Sequence Number
Biometric
PIN
Response Key
Message Key
Seller Code
Message Data
MAC
Commercial Transaction Request Message
Begin Decrypt and Validate at DPC
Identify BIA from VAD using Hardware ID
Validate Sequence Number
Get next DUKPT Key using Sequence Number
Decrypt message using DUKPT Key
Calculate MAC for message using MAC Key
Compare MAC with MAC stored in message
Identify Apparatus Owner using Seller ID
Validate Seller Code in message
Retrieve Seller Financial Account from AOD Record
Decrypt and Validate at DPC Complete
Hardware ID
Sequence Number
DUKPT Key Table
MAC Key
Seller ID
VAD Record
Seller ID
Seller Code
Financial Account
AOD Record
Valid Apparatus Database (VAD)
Apparatus Owner Database (AOD)

FIG. 8

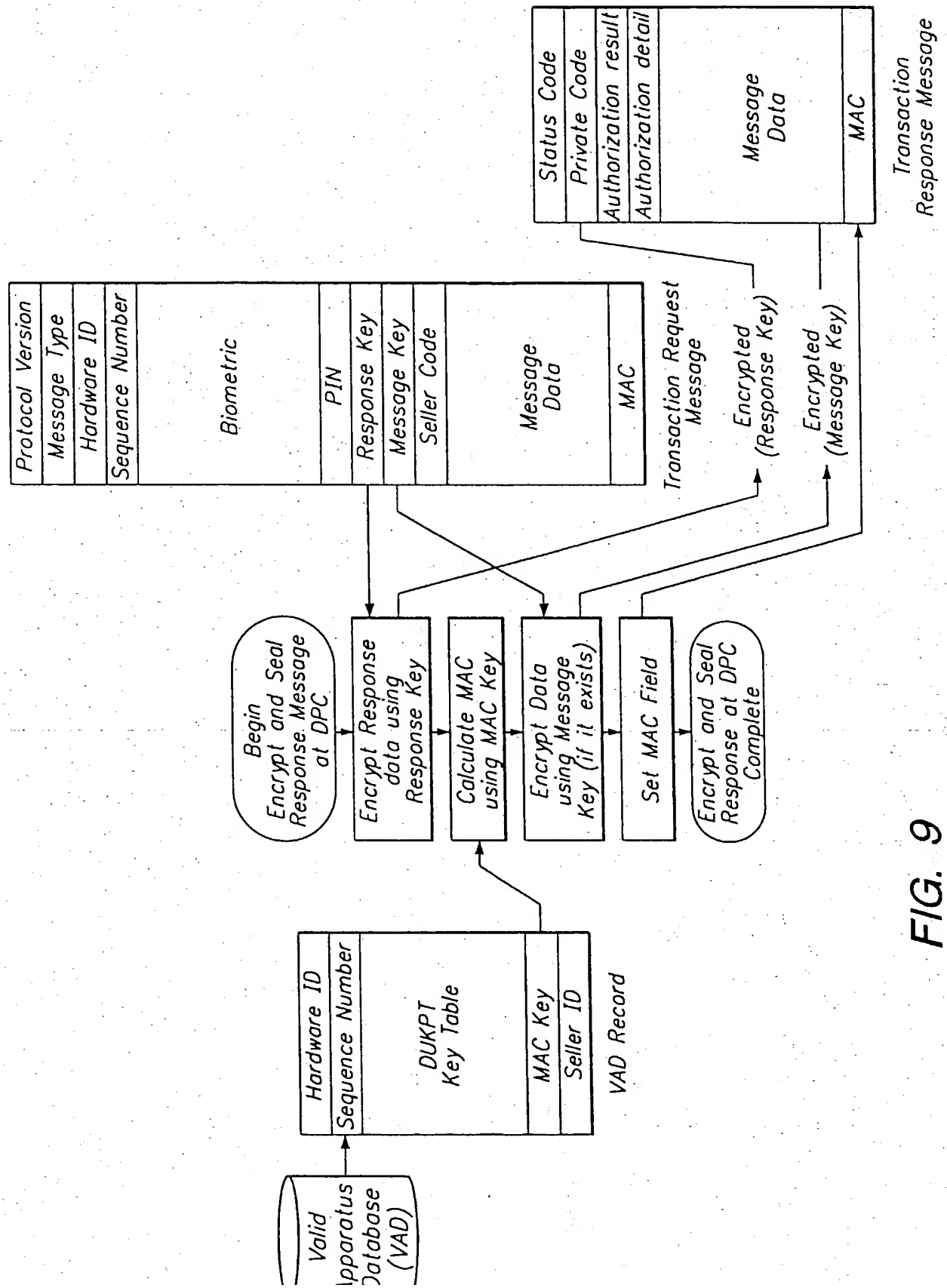
Valid Apparatus Database (VAD)
Hardware ID
Sequence Number
DUKPT Key Table
MAC Key
Seller ID
VAD Record
Begin Encrypt and Seal Response Message at DPC
Encrypt Response data using Response Key
Calculate MAC using MAC Key
Encrypt Data using Message Key (if it exists)
Set MAC Field
Encrypt and Seal Response at DPC Complete
Protocol Version
Message Type
Hardware ID
Sequence Number
Biometric
PIN
Response Key
Message Key
Seller Code
Message Data
MAC
Transaction Request Message
Encrypted (Response Key)
Encrypted (Message Key)
Status Code
Private Code
Authorization result
Authorization detail
Message Data
MAC
Transaction Response Message

FIG. 9

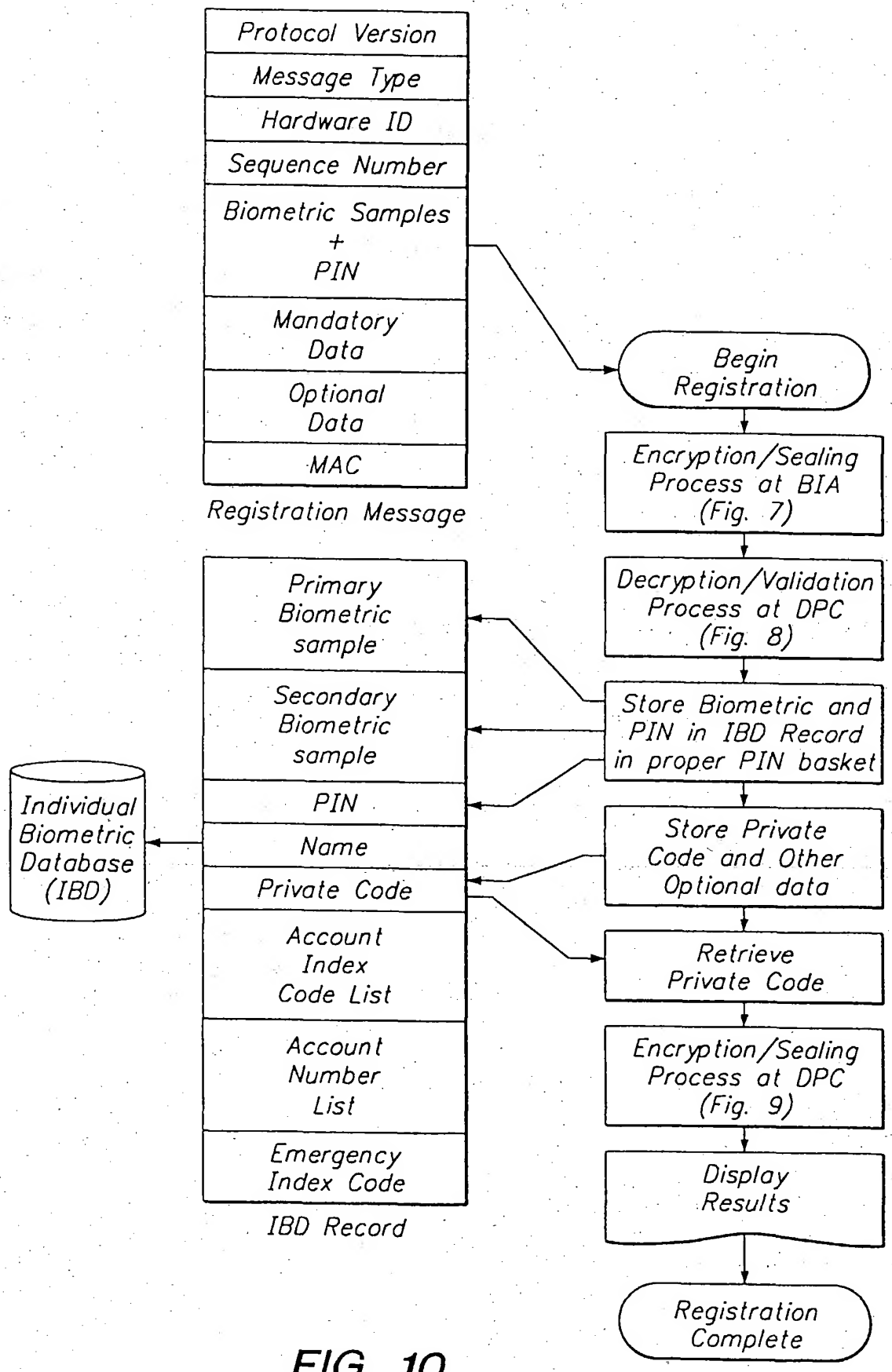
Protocol Version
Message Type
Hardware ID
Sequence Number
Biometric Samples + PIN
Mandatory Data
Optional Data
MAC
Registration Message
Begin Registration
Encryption/Sealing Process at BIA (Fig. 7)
Decryption/Validation Process at DPC (Fig. 8)
Store Biometric and PIN in IBD Record in proper PIN basket
Store Private Code and Other Optional data
Retrieve Private Code
Encryption/Sealing Process at DPC (Fig. 9)
Display Results
Registration Complete
Primary Biometric sample
Secondary Biometric sample
PIN
Name
Private Code
Account Index Code List
Account Number List
Emergency Index Code
IBD Record
Individual Biometric Database (IBD)

FIG. 10

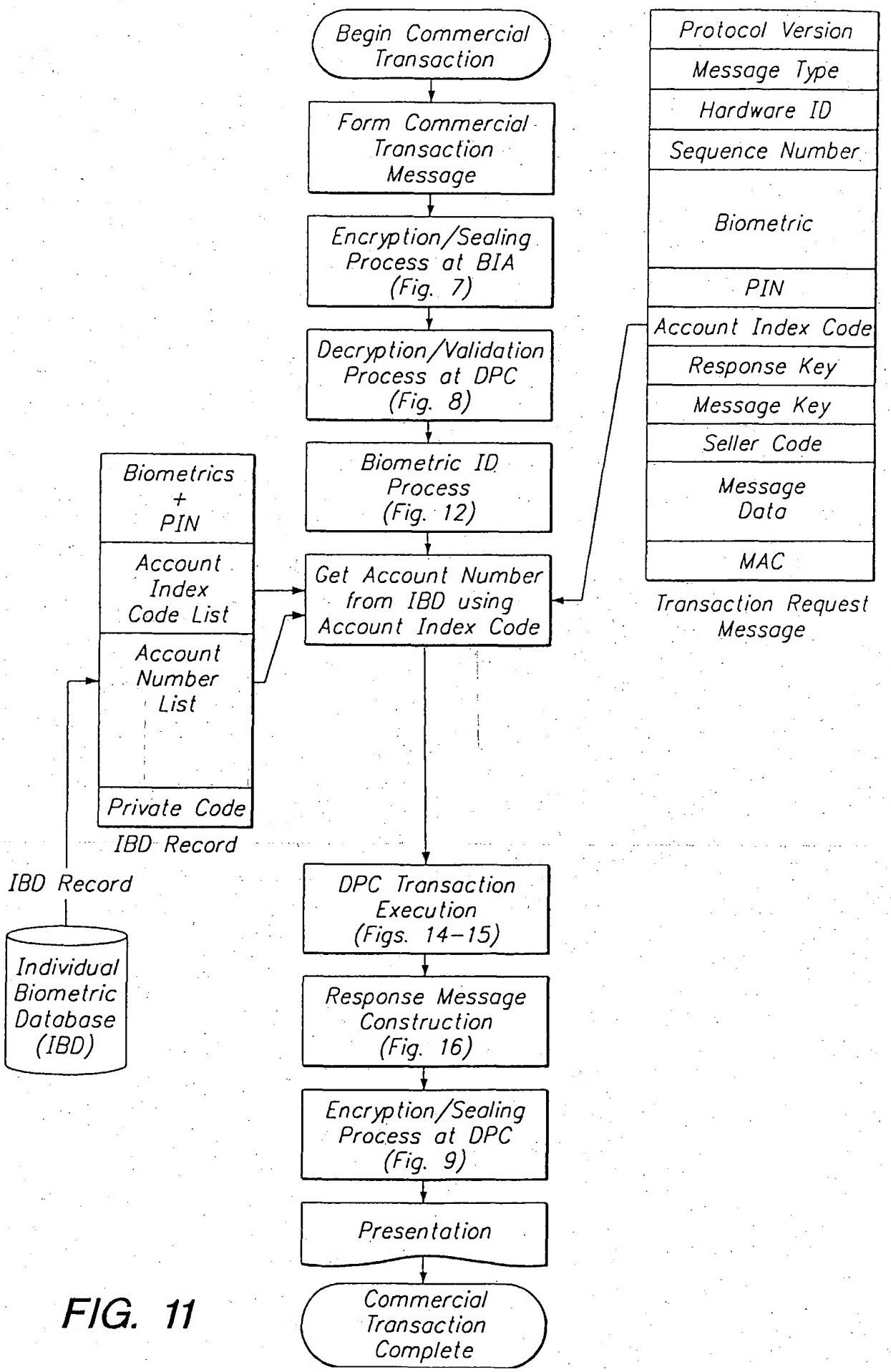
Begin Commercial Transaction
Form Commercial Transaction Message
Encryption/Sealing Process at BIA (Fig. 7)
Decryption/Validation Process at DPC (Fig. 8)
Biometric ID Process (Fig. 12)
Get Account Number from IBD using Account Index Code
DPC Transaction Execution (Figs. 14–15)
Response Message Construction (Fig. 16)
Encryption/Sealing Process at DPC (Fig. 9)
Presentation
Commercial Transaction Complete
Protocol Version
Message Type
Hardware ID
Sequence Number
Biometric
PIN
Account Index Code
Response Key
Message Key
Seller Code
Message Data
MAC
Transaction Request Message
Biometrics + PIN
Account Index Code List
Account Number List
Private Code
IBD Record
IBD Record
Individual Biometric Database (IBD)

FIG. 11

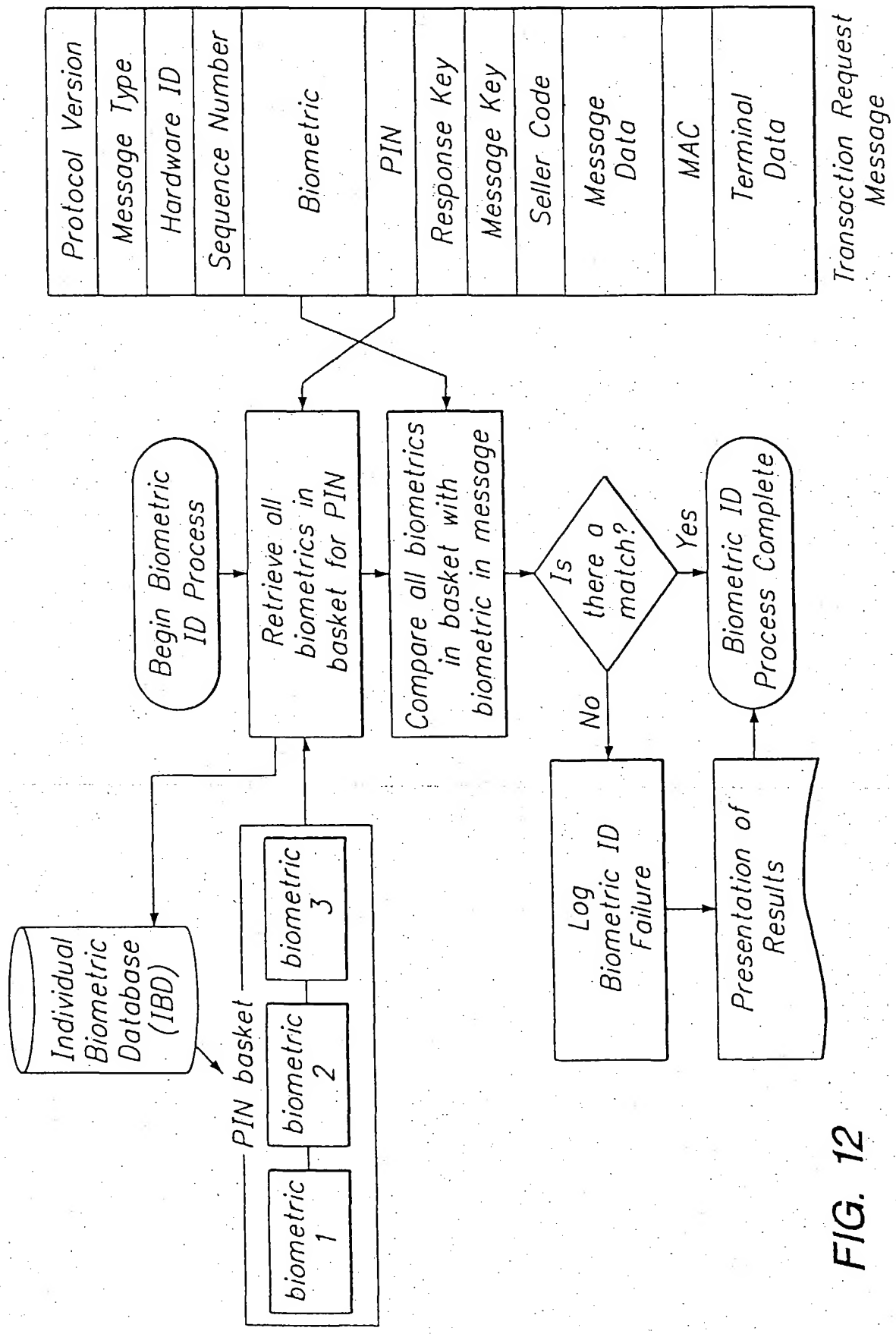
Protocol Version
Message Type
Hardware ID
Sequence Number
Biometric
PIN
Response Key
Message Key
Seller Code
Message Data
MAC
Terminal Data
Transaction Request Message
Begin Biometric ID Process
Retrieve all biometrics in basket for PIN
Compare all biometrics in basket with biometric in message
Is there a match?
Yes
No
Biometric ID Process Complete
Log Biometric ID Failure
Presentation of Results
Individual Biometric Database (IBD)
PIN basket
biometric 1
biometric 2
biometric 3

FIG. 12

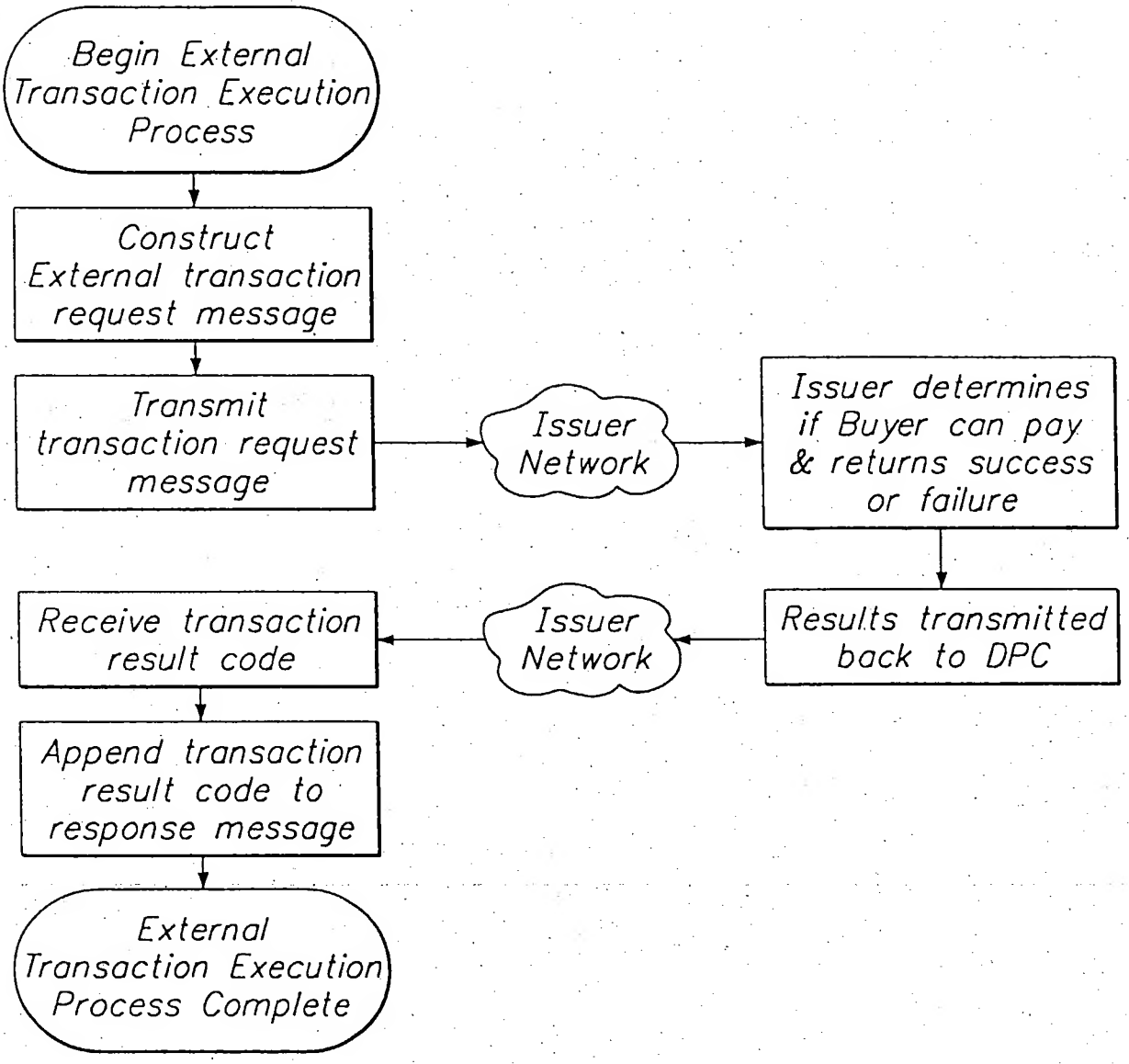
Begin External Transaction Execution Process
Construct External transaction request message
Transmit transaction request message
Issuer Network
Issuer determines if Buyer can pay & returns success or failure
Results transmitted back to DPC
Issuer Network
Receive transaction result code
Append transaction result code to response message
External Transaction Execution Process Complete

FIG. 13

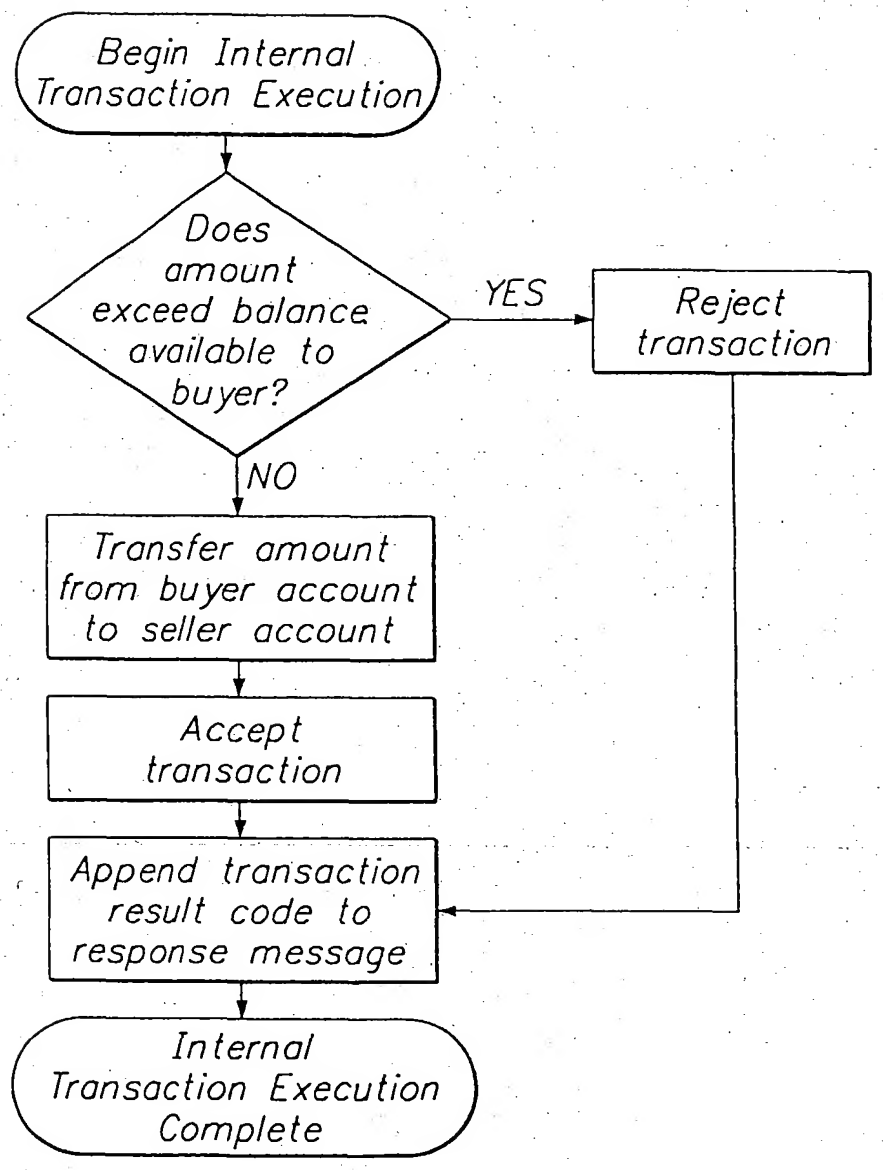
Begin Internal Transaction Execution
Does amount exceed balance available to buyer?
YES
Reject transaction
NO
Transfer amount from buyer account to seller account
Accept transaction
Append transaction result code to response message
Internal Transaction Execution Complete

FIG. 14

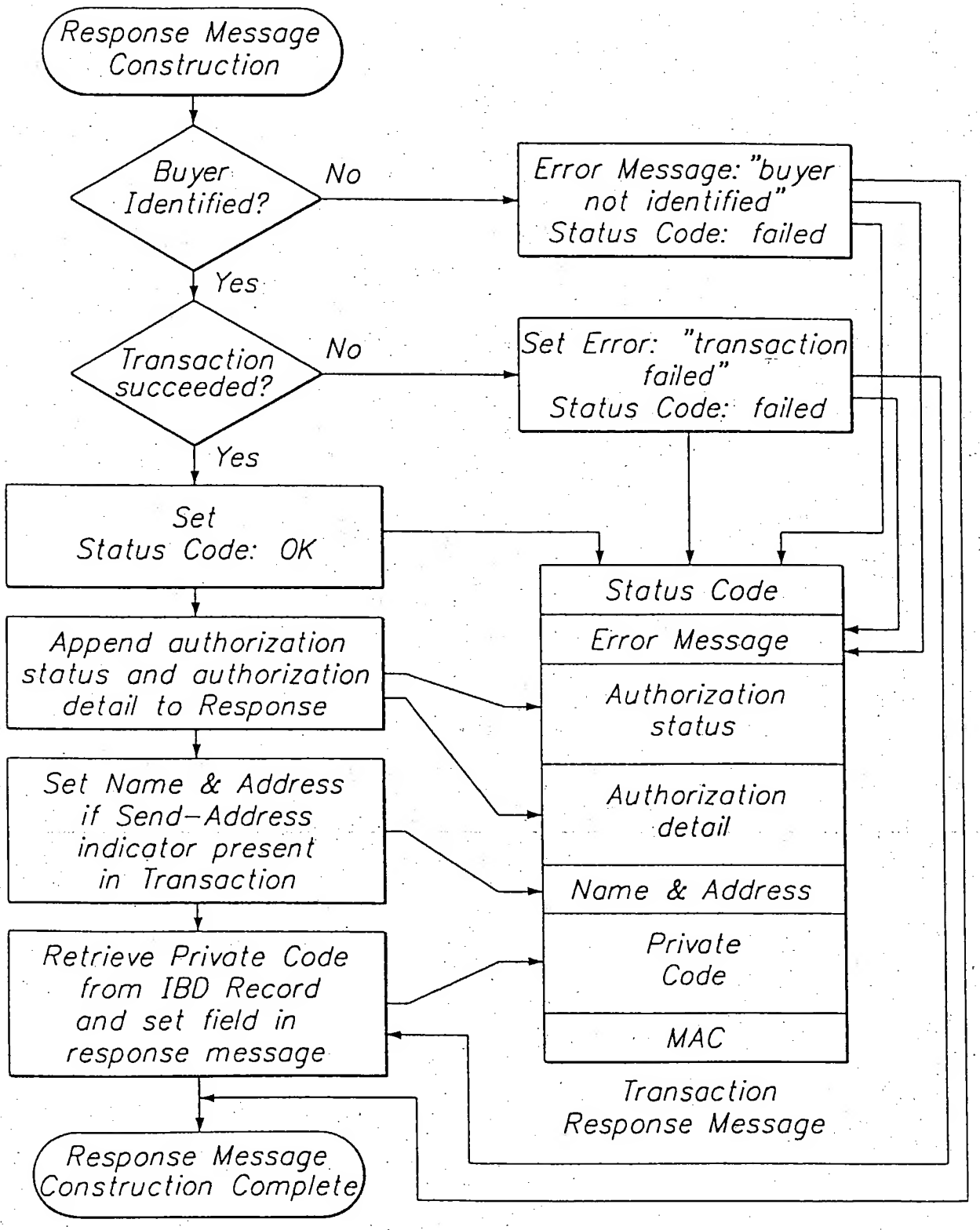
Response Message Construction
Buyer Identified?
No
Error Message: "buyer not identified" Status Code: failed
Yes
Transaction succeeded?
No
Set Error: "transaction failed" Status Code: failed
Yes
Set Status Code: OK
Append authorization status and authorization detail to Response
Set Name & Address if Send-Address indicator present in Transaction
Retrieve Private Code from IBD Record and set field in response message
Response Message Construction Complete
Status Code
Error Message
Authorization status
Authorization detail
Name & Address
Private Code
MAC
Transaction Response Message

FIG. 15

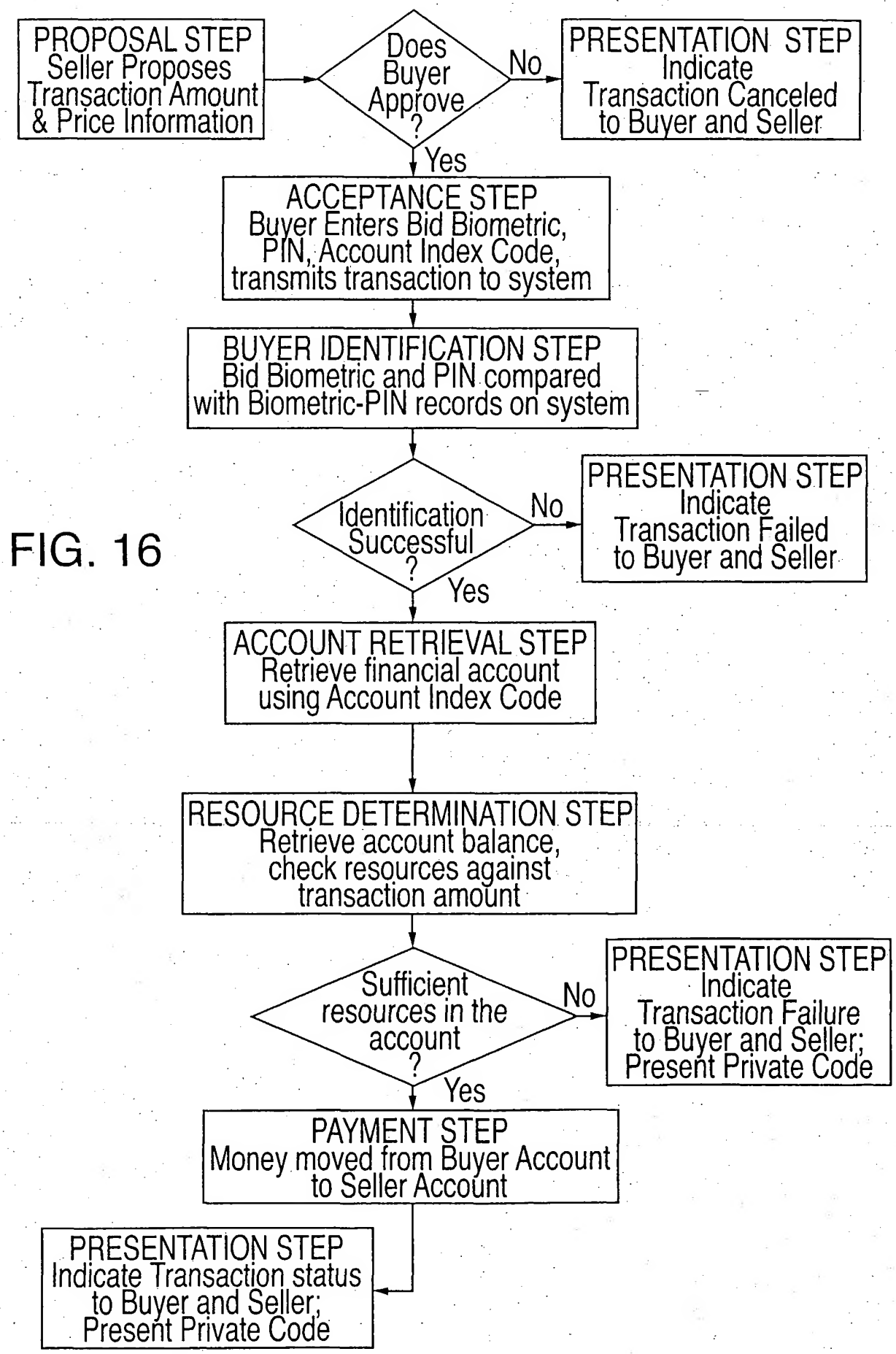
PROPOSAL STEP
Seller Proposes Transaction Amount & Price Information
Does Buyer Approve ?
No
PRESENTATION STEP
Indicate Transaction Canceled to Buyer and Seller
Yes
ACCEPTANCE STEP
Buyer Enters Bid Biometric, PIN, Account Index Code, transmits transaction to system
BUYER IDENTIFICATION STEP
Bid Biometric and PIN compared with Biometric-PIN records on system
Identification Successful ?
No
PRESENTATION STEP
Indicate Transaction Failed to Buyer and Seller
Yes
ACCOUNT RETRIEVAL STEP
Retrieve financial account using Account Index Code
RESOURCE DETERMINATION STEP
Retrieve account balance, check resources against transaction amount
Sufficient resources in the account ?
No
PRESENTATION STEP
Indicate Transaction Failure to Buyer and Seller; Present Private Code
Yes
PAYMENT STEP
Money moved from Buyer Account to Seller Account
PRESENTATION STEP
Indicate Transaction status to Buyer and Seller; Present Private Code

FIG. 16